Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 22 March 2004

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
www.whitehouse.gov/homeland

Daily Overview

- The San Diego Union−Tribune reports San Diego State University is warning more than 178,000 students, alumni and employees that hackers broke into a university computer server where names and Social Security numbers were stored. (See item 7)

- US Newswire reports the possibility of new terrorist attacks in the U.S., perhaps including the use of a radiological dispersion device as well as poisons and chemicals, has underlined the need for medical professionals to plan for a radiological terrorist attack. (See item 18)

- The Washington Post reports that the quickly spreading Witty worm destroyed or damaged tens of thousands of personal computers worldwide Saturday morning by exploiting a security flaw in a firewall program. (See item 23)

- Internet Security Systems has raised AlertCon to Level 2, due to increased threat from Witty worm activity. Please refer to the Internet Alert Dashboard.

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical; Defense Industrial Base

Service Industries: Banking and Finance; Transportation; Postal and Shipping

Sustenance and Health: Agriculture; Food; Water; Public Health

Federal and State: Government; Emergency Services

IT and Cyber: Information and Telecommunications; Internet Alert Dashboard

Other: General; DHS/IAIP Web Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *March 19, Courier−Post (NJ)* — **Utility promises nuclear reforms.** The operator of the Salem nuclear−power complex on Thursday, March 18, gave itself poor marks in encouraging

employees to raise safety and equipment concerns. PSEG Nuclear officials acknowledged its shortcomings during a meeting with the federal Nuclear Regulatory Commission (NRC). In January, the NRC sent a letter to PSEG expressing concerns about the station's "work environment, particularly as it relates to the handling of emergent equipment issues and associated operational decision making." Thursday's meeting allowed the company to begin outlining its response plan. **Company officials said it will take years to completely fix its work environment problems, but said they have launched numerous measures toward that end, including independent reviewers who are interviewing employees to determine the cause of problems. PSEG Power, parent company to PSEG Nuclear, also plans to invest $648 million to upgrade the "material condition" of the Hope Creek and twin Salem reactors over the next five years,** said Frank Cassidy, president and chief operating officer for PSEG Power. Located on Artificial Island, NJ, the Hope Creek and Salem 1 and Salem 2 reactors are the nation's second−largest nuclear complex and generate more than half the electricity PSEG produces.
Source: http://www.courierpostonline.com/news/southjersey/m031904g.h tm

2. *March 19, Dow Jones Business News* — **NRC must study terror threat to nuclear project says attorney general. California Attorney General Bill Lockyer Friday, March 19, filed an amicus brief in federal court urging the U.S. Nuclear Regulatory Commission (NRC) to evaluate the effects a terrorist attack would have on a nuclear fuel storage facility proposed by Pacific Gas & Electric.** The PG&E Corp. unit is looking to expand spent fuel storage capacity at its 2,200 megawatt Diablo Canyon Nuclear Plant near San Luis Obispo, CA. The utility expects a decision from the NRC soon on whether it can proceed with the project, which it hopes to complete in 2006, said Pacific Gas & Electric spokesperson Jeff Lewis. **The NRC ruled in January 2003 that it didn't have to address potential terrorism in its environmental assessment of the facility, a position which endangers California residents, Lockyer said.** Lockyer's friend−of−the−court brief, filed at the U.S. Ninth Circuit Court of Appeals, asks that the NRC be ordered to conduct a study on the effects of a possible terrorist attack, and to hold public hearings in the process. The NRC has strict requirements for building storage facilities, which studies have shown can withstand the impact of a commercial aircraft, Lewis said.
Source: http://biz.yahoo.com/djus/040319/1603000844_1.html

3. *March 18, Dow Jones Business News* — **Texas grid monitor approves new power line projects.** The board of the organization that oversees the transmission system in most of Texas approved this week a $200 million proposal to build two power connections with Mexico aimed at maintaining the electric system in the southern part of the state. **The plan the Ercot board approved Wednesday, March 18, involves building a 345−kilovolt transmission line from the San Miguel Power Plant south of San Antonio to the Highway 59 substation near Laredo. It also includes the construction of a 150− megawatt direct current tie with Mexico's utility, Commission Federal de Electricidad.** Several transmission system improvements are scheduled to be completed in the region this year, but the power monitor said additional projects are needed to ensure supply keeps pace with growing demand. Though the yearly estimated cost to consumers of the new transmission line remains the same, the new cable is needed to prevent blackouts due to supply shortages, Ercot Director of Transmission Services Bill Bojorquez said. Ercot has projected power interruptions could occur by 2013 without it. The link with Mexico will likely require the approval of Mexico's government, and

the transmission line will require the go−ahead from Texas utility regulators, Ercot CEO Sam Jones said.
Source: http://biz.yahoo.com/djus/040318/1744001180_1.html

[Return to top]

Chemical Sector

4. *March 20, South Bend Tribune* — **Chemical cloud forces plant employees to evacuate.** More than a dozen workers in Kingsbury, IN, were taken to LaPorte Hospital on Friday, March 20, morning due to a vapor cloud inside the plant formed by mishandling of chemicals. About 6:30 a.m., emergency personnel from various departments in LaPorte County responded to National Products at the Kingsbury Industrial Park. A delivery of 5,000 gallons of a liquid bleach solution had arrived in a tanker truck from Chicago, said LaPorte County Hazardous Materials Team Director Roger Wolff. The driver began pumping the bleach from the tanker into a single line connected to hoses leading to six 3,000−gallon tanks. **Each of the tanks, however, contained hydrochloric acid and when mixed with bleach from the truck there was a chemical reaction producing a vapor cloud inside the plant, said Wolff. "Those products then reacted with each other and created hydrochloric fumes and chlorine vapors," said Wolff.** After roughly 500 gallons of bleach had been pumped from the tanker, the driver noticed a vapor cloud forming above the storage tanks and stopped the flow, said Wolff. The load was supposed to be pumped into tanks containing bleach at another National Products building at the Kingsbury Industrial Park about a mile away, said Wolff. All of the approximately 35 workers in the building were evacuated.
Source: http://www.southbendtribune.com/stories/2004/03/20/local.200
40320−sbt−MARS−A6−Chemical_cloud_force.sto

[Return to top]

Defense Industrial Base Sector

5. *March 19, Government Computer News* — **DoD tries out biometric smart cards overseas.** The Department of Defense's (DoD) broadest smart card rollout for biometric authentication is happening in South Korea, Japan and Europe−not the United States, Kenneth C. Scheflen said. Scheflen, director of the Defense Manpower Data Center, said the pieces "are not all there yet for an enterprise biometric solution." Vendors' products are still closed to interoperability, he said, and the algorithms used for fingerprint comparison remain proprietary. Although DoD continues to push vendors toward an interoperable smart−card business model, it has managed "to badge individuals without DoD credentials in the largest biometric access program in the department," Scheflen said. **The Defense Biometric Identification System, or DBIDS, places a digital fingerprint and photo on a smart card in a scalable configuration that local authorities can adapt to their requirements. The card goes to individuals who do not qualify for DoD's Common Access Card.** "The DBIDS fingerprint database refreshes daily" from a central database server to notebook computers at local checkpoints, Scheflen said. So far, there are about 650,000 military users and contractors registered in DBIDS at European sites, Japan, Kuwait and the Naval Postgraduate School at Monterey, CA.

Source: http://www.gcn.com/vol1_no1/daily−updates/25350−1.html

6. *March 17, General Accounting Office* — **GAO−04−530T: Unmanned Aerial Vehicles: Major Management Issues Facing DOD's Development and Fielding Efforts (Testimony).** The current generation of unmanned aerial vehicles (UAVs) has been under development since the 1980s. UAVs were used in Afghanistan and Iraq in 2002 and 2003 to observe, track, target, and strike enemy forces. These successes have heightened interest in UAVs within the Department of Defense (DoD). **Congress has been particularly interested in DoD's approach to managing the growing number of UAV programs.** The General Accounting Office (GAO) was asked to summarize (1) the results of its most current report on DoD's approach to developing and fielding UAVs and the extent to which the approach provides reasonable assurance that its investment will lead to effective integration of UAVs into the force structure, and (2) the major management issues GAO has identified in prior reports on UAV research and development. In our most recent report, **GAO recommends that DoD (1) establish a strategic plan to guide UAV development and fielding and (2) designate the UAV Task Force or other appropriate body to oversee the plan's implementation, ensuring sufficient authority is provided.** Highlights: http://www.gao.gov/highlights/d04530thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−04−530T

[Return to top]

Banking and Finance Sector

7. *March 17, San Diego Union−Tribune* — **Personal data at risk, thousands are warned. San Diego State University (SDSU) is warning more than 178,000 students, alumni and employees that hackers broke into a university computer server where names and Social Security numbers were stored.** The university began mailing out notification letters Monday, March 15, urging people whose personal information was on the server to get copies of their credit reports and review them for suspicious activity. **University officials said the hackers infiltrated a server in the Office of Financial Aid and Scholarships in late December and used it to send spam e−mail messages and transfer files.** The problem was discovered in the last week of February and SDSU took the server off the network. The server contained financial aid reports since 1998, but not the applications themselves or award information. SDSU said there is no indication that the intruders targeted confidential information in the system. "We have to let people know what happened and let them take steps to protect themselves." The case is being investigated by university police. The FBI also has been notified because there is evidence that the hackers broke into the server from another state, said SDSU police Capt. Steve Williams.
Source: http://www.signonsandiego.com/news/computing/20040317−9999−news_7m17hacker.html

[Return to top]

Transportation Sector

8. *March 21, Star Telegram (Ft. Worth, TX)* — **Remote−control trains' safety is questioned. The Brotherhood of Locomotive Engineers and Trainmen says remote−control locomotives are dangerous because they take one of the human operators out of the equation.** Throwing the debate into starker relief, the east Arlington, TX, switch−yard that is now using remote−control locomotives is the same one where an accident in December 2002 caused a derailment that left a railcar dangling over Texas highway 360. **The union is lobbying for federal regulations that would require operators to see in front of the cars they are pushing, among other rules. Currently, the Federal Railroad Administration offers only recommendations for the use of remote control locomotives −− not requirements.** About 30 U.S. cities, such as Shreveport, LA, have banned the use of remote−control switch engines until more safety considerations are put into place.
Source: http://www.dfw.com/mld/dfw/news/local/states/texas/arlington /8226606.htm

9. *March 19, Sunday Herald (UK)* — **Royal Navy urged to protect ships from piracy raids.** The UK government is facing growing pressure to provide Royal Navy patrols to protect merchant vessels against international piracy on the high seas. Amid growing fears for their members' safety, mariners' union Numast is urging the government to recognize that the global shipping trade is a soft target for pirates and terrorists, and that the Royal Navy should be engaged in convoys to protect British interests at sea. **Numast's Andrew Linington said that 90% of world trade moves by sea, providing rich and easy pickings. But there is also a "huge" potential terrorist threat posed by the environmental impact of a deliberate tanker spill or a gas or chemical tanker being used as a floating bomb, either of which are "very real scenarios."** The frequency of pirate attacks and the level of violence used have steadily increased over the last 10 years. In 2003, 445 incidents were reported, in which 21 seafarers died and 71 passengers and crew went missing, according to the International Maritime Bureau's Piracy Reporting Center. **The waters off Indonesia, particularly the Malacca Straits, are a notorious hot spot, although incidents occur off Africa, India, the Americas and elsewhere.**
Source: http://www.sundayherald.com/40671

10. *March 19, Houston Chronicle* — **Tanker, two barges collide in Houston Ship Channel.** The Houston Ship Channel was closed for nearly four hours Friday afternoon, March 19, after an 800−foot tanker collided with a tugboat pushing two barges, causing about 500 barrels of a high−octane petroleum product to spill, the Coast Guard said. All five people aboard the tug, David and Colleen, were accounted for with no injuries. Coast Guard officials said the leak was plugged and the spilled petroleum was evaporating and not likely to cause an environmental hazard. "It's similar to gasoline. It has a high evaporation point," said Petty Officer Nick Cangemi of the spilled substance, called raffinate, that leaked from one barge. The incident occurred around 2:15 p.m. just north of where the channel meets the Gulf Intracoastal Waterway, not far from the Texas City Dike. **The junction is one of the world's busiest ship and barge traffic intersections, said Capt. Alistair Macnab, president of the Greater Houston Port Bureau. From here, ships take products to the ports of Texas City, Galveston and Houston.**
Source: http://www.chron.com/cs/CDA/ssistory.mpl/metropolitan/245827 0

11. *March 19, The Trucker* — **ATA endorses plans to make railcars more visible.** Plans by the Federal Railroad Administration (FRA) to make all rolling stock more visible have drawn the

support of the American Trucking Associations (ATA). In a written endorsement for the ATA in Alexandria, VA, S.W. Gouse III, vice president of Engineering, stated that "improved railcar conspicuity will save lives." Most railroad rolling stock currently in use isn't marked with "retroflective tape or any sort of illumination or reflectivity, and many are dark in color, which limits the capability of motorists "to see rail cars under many lighting conditions," Gouse stated. **He pointed out that crash data collected from about 11,000 accidents involving tractor−trailers for two years beginning in 1997 "conclusively proved" that the use of high visibility tape resulted in a 37 percent drop in side and rear−end accidents in Florida alone, and a 44 percent decline in Pennsylvania.** The ATA is encouraging the FRA to, once the rulemaking process is complete, "require lighting on railcars similar to that required on trucks, truck trailers and intermodal chassis to further enhance highway safety." From 1983 to 1992, there was an annual average of 583 fatalities and "tens of thousands of additional injuries," Gouse stated, resulting from railcars colliding with motor vehicles.
Source: http://www.thetrucker.com/stories/03_04/0319_rail_reflectors .html

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

12. *March 19, Agriculture Online* — **Industry−wide BSE summit slated for late April. Finding a unified approach to handling the multiple facets of bovine spongiform encephalopathy (BSE) in North America will be the focus of a BSE summit in Fort Worth, Texas April 26−27.** Members of the checkoff−funded Beef Industry Food Safety Council (BIFSCo) are modeling the meeting after a summit on E. coli O157:H7 that took place last year. BIFSCo members hope to attract their counterparts from the Canadian and Mexican industries to the April meeting, as well as the U.S. federal agencies working on the BSE issue. Invitations will be extended to representatives from every industry segment touched by the BSE situation, including the rendering, feed and dairy industries. The goal of the meeting, coordinated on behalf of the Cattlemen's Beef Board and state beef councils by the National Cattlemen's Beef Association (NCBA), will be to identify where more knowledge and research is needed and establish best practices to strengthen defenses against this disease.
Source: http://www.agriculture.com/default.sph/AgNews.class?FNC=goDe tail__ANewsindex_html___51460___1

13. *March 19, AgProfessional* — **Soybean aphids may not be as bad as 2004.** Some early season clues suggest that soybean aphids may not be quite as troublesome for Midwestern farmers this season as they were in 2003. **University of Illinois extension entomologist Kevin Steffey bases this assertion on a network of suction traps established to monitor the soybean pest, which first invaded the U.S. in July 2000.** "It is interesting to note that very few aphids were captured in the suction traps during the fall of 2003," he said. "The presence or relative absence of the multicolored Asian lady beetle, the primary predator of soybean aphids, also may play a

role in regulating populations of soybean aphids." "The relatively low numbers of soybean aphids captured in suction traps in the fall of 2003 and the presence of very large numbers of multicolored Asian lady beetles suggest that soybean aphids may not get off to a fast start in 2004," he said. Soybean aphid populations thrive when conditions are relatively cool, while their population growth slows when temperatures are high. Conditions in 2003 were favorable for the growth and development of the pest, which may produce as many as 18 generations in a single season.
Source: http://www.agprofessional.com/show_story.php?id=24174

14. *March 19, AgProfessional* — **Canadian farmers see growing opposition to GM wheat.** Opposition to growing genetically modified (GM) wheat in Canada is increasing, said Ken Ritter, Chairman of the Canadian Wheat Board's farmer−controlled board of directors. **Speaking to farmers and industry representatives in Calgary on Thursday, March 18, Ritter said 87 percent of the customers who purchase wheat produced by western Canadian farmers require that the CWB provide guarantees the wheat is not genetically modified. This was up from 82 percent just two years ago.** "We're seeing increasing concern and opposition from our customers over the introduction of GM wheat," Ritter said. "As a farmer, what concerns me the most is that the markets resistant to GM wheat include all of the markets where the CWB usually achieves a premium." The loss of these markets would have a disproportionate impact on farmers' incomes, Ritter said. "We've all witnessed the devastation a single case of BSE has caused in Canada's beef industry. The introduction of GM wheat could cause similar devastation in our wheat industry," he said.
Source: http://www.agprofessional.com/show_story.php?id=24164

[Return to top]

Food Sector

15. *March 19, San Diego Union−Tribune* — **Mexican candy pulled from local shelves. San Diego County, CA, health officials are pulling the candy Chaca Chaca from local markets after the U.S. Food and Drug Administration (FDA) banned the Mexican product from entering the United States on Thursday, March 18. The FDA's "import alert," which authorizes U.S. border inspectors to stop shipments of Chaca Chaca, was issued because the candy contains levels of lead that could be harmful to infants, children and pregnant women,** said Joe Baca, compliance director for the FDA's Center for Food Safety and Applied Nutrition. Gilberto Chavez, associate director and state epidemiologist of the California Department of Health Services, also issued a warning against consumption of the product. Chaca Chaca, a confection of peach, apple and mango pulp mixed with salt and chile, is made by Industrial Dulcera based in Morelia, Michoacan. It is typically sold in small markets. The source of lead in the candy has not been identified, Baca said. It could result from how it is stored or wrapped, or from one of its ingredients.
Source: http://www.signonsandiego.com/news/metro/20040319−9999−news_1m19chaca.html

16. *March 19, The Food and Drug Administration and the Environmental Protection Agency* — **FDA and EPA announce the revised consumer advisory on methylmercury in fish. The Food and Drug Administration (FDA) and the Environmental Protection Agency (EPA) announced on Friday, March 19, their joint consumer advisory on methylmercury in fish**

and shellfish for reducing the exposure to high levels of mercury in women who may become pregnant, pregnant women, nursing mothers, and young children. This unifies advice from both FDA and EPA and supercedes FDA's and EPA's 2001 advisories. By following these three recommendations for selecting and eating fish or shellfish, women will receive the benefits of eating fish and shellfish and be confident that they have reduced their exposure to the harmful effects of mercury: 1) Do not eat Shark, Swordfish, King Mackerel, or Tilefish because they contain high levels of mercury; 2) Eat up to 12 ounces (two average meals) a week of a variety of fish and shellfish that are lower in mercury; and 3) Check local advisories about the safety of fish caught by family and friends in your local lakes, rivers and coastal areas.
Source: http://www.fda.gov/bbs/topics/news/2004/NEW01038.html

[Return to top]

Water Sector

17. *March 18, Casa Grande Valley Newspaper (AZ)* — **Town has enough water for 60,000 people, but population expected to grow.** A just released report on the city Florence, AZ's 100−year water supply shows that there's enough to go around, but that the city could experience shortage around 2020. The study said that there will be enough water sufficient for 60,000 residents. However, Public Works Director Wayne Costa said population projections for the year 2020 show there could be as many as 70,000 people in the town's water service area, with 49,000 people living in the Merrill Ranch development, which was recently annexed. The state Department of Water Resources requires a 100−year assured water supply for all subdivided lands for sale or lease located in an active management area. **In a state and an area that continues to suffer from drought conditions, Randy Edmond, acting director of the Arizona Department of Water Resources' Pinal Active Management area has recently expressed concerns about how this groundwater is being replenished.** The average home now uses about 200 gallons of water a day in Pinal County. Florence is just one city among many in Pinal County labeled a growth area.
Source: http://www.zwire.com/site/news.cfm?newsid=11144449&BRD=1817&PAG=461&dept_id=222076&rfi=6

[Return to top]

Public Health Sector

18. *March 19, US Newswire* — **American College of Radiology resource prepares medical professionals for radiological terrorist attack.** A year of heightened terrorism alerts, repeated government warnings of the likelihood of new terrorist attacks in U.S., possibly including the “use of a radiological dispersion device as well as poisons and chemicals,” and recent terrorist attacks abroad has underlined the need for radiology professionals to plan ahead. **In response to this need, the American College of Radiology (ACR), in conjunction with the American Society of Therapeutic Radiology and Oncology and the American Association of Physicists in Medicine, has created a primer entitled “Disaster Preparedness for Radiology Professionals: Response to Radiological Terrorism,” a readily available**

resource to help medical professionals and emergency personnel better manage an emergency situation resulting from a radiological disaster or terrorist attack. The primer, which can be downloaded directly from the ACR Web site at http://www.acr.org via a direct link, Disaster Planning Information (bottom−left of page), serves as a quick reference in the event of a radiological event and offers guidance on proper preparation, as well as directives on handling contaminated persons and consequences of radiation exposure. The primer also includes information on radiological findings related to agents that could be used in a biological or chemical attack.
Source: http://releases.usnewswire.com/GetRelease.asp?id=122−0319200 4

19. *March 19, United Press International* — **WHO warns of lax flu epidemic preparations.** Despite warnings the recent Avian bird flu outbreak in Asia signifies another influenza pandemic could be imminent, governments worldwide are behind in preparations and need to intensify their efforts, the chief of the World Health Organization (WHO) warned. **"We know another pandemic is inevitable. It is coming, and when this happens, we also know that we are unlikely to have enough drugs, vaccines, healthcare workers and hospital capacity to cope," Dr. Lee−Wook Lee, WHO's director−general told more than 100 health experts Thursday at the end of a three−day influenza pandemic preparedness meeting.** Epidemiological models, according to WHO scientists, project influenza pandemic in industrialized countries alone would result in 57 million to 132 million outpatient hospital visits, plus one million to 2.3 million admissions and between 280,000 to 650,000 deaths in less than two years. The impact in poor nations would be far greater, however, because healthcare resources already are strained and scarce, they add. Some of the biggest gaps in readiness, however, involve limitations in the manufacturing capacity and availability of antivirals, which are essential in the early stages.
Source: http://www.upi.com/view.cfm?StoryID=20040319−080018−9509r

[Return to top]

Government Sector

Nothing to report.

[Return to top]

Emergency Services Sector

20. *March 19, New Scientist* — **Defusing fertilizer may make bomb−building harder.** Vigilance and intelligence will always be the best weapons against terrorism. But it may possible to make it harder for terrorists to turn one readily available chemical into bombs. **Ammonium nitrate, a widely used fertilizer, has been used in several IRA attacks, the World Trade Center bombing in New York in 1993, the Oklahoma City bombing in 1995 and the Bali bombing in 2002. The massive bomb found outside the U.S. embassy in Karachi, Pakistan also contained the chemical, according to some reports.** Millions of tons of ammonium nitrate are produced each year for use as a fertilizer. **Now a company based in Belton, MO, is patenting a water−soluble polymer coating for the fertilizer granules that repels fuel oil. The coating dissolves rapidly in soil, so it would not interfere with ammonium nitrate's main function**

as fertilizer. If it works and is widely adopted, the treatment could make it harder for terrorists to turn grade−grade ammonium nitrate into bombs, and could also help prevent industrial accidents.
Source: http://www.newscientist.com/news/news.jsp?id=ns99994782

21. *March 19, New York Times* — **Addressing the unthinkable, U.S. revives study of fallout.** To cope with the possibility that terrorists might someday detonate a nuclear bomb on American soil, the federal government is reviving a scientific art that was lost after the cold war: fallout analysis. **The goal, officials and weapons experts both inside and outside the government say, is to figure out quickly who exploded such a bomb and where the nuclear material came from.** That would clarify the options for striking back. Officials also hope that if terrorists know a bomb can be traced, they will be less likely to try to use one. **The government is also building robots that would go into an affected area and take radioactive samples, as well as field stations that would dilute dangerous material for safe shipment to national laboratories.** "Certainly, there's a frightening aspect in all of this," said Charles B. Richardson, the project leader for nuclear identification research at the Sandia National Laboratories in Albuquerque. "But we're putting all these things together with the hope that they'll never have to be used."
Source: http://www.nytimes.com/2004/03/19/national/19NUKE.html?th

22. *March 19, The Honolulu Advertiser* — **Hawaii struggles with security. Federal mandates, paperwork and money problems are overwhelming Hawaii homeland security officials as they struggle to secure airports and ports and improve communication among emergency responders.** "We have grave concerns about homeland security," said Doug Aton, director of Honolulu's Civil Defense. It could take several years before Hawaii meets federal requirements for security and cooperation among first responders — police, fire, hazardous materials teams and other agencies. When first responders can't communicate effectively "it can literally cost lives," the General Accounting Office said late last year. Pressure is mounting on local officials to prioritize their needs, apply for a long list of complex federal grants and develop strategies for spending the money. They also must train first responders and create tracking systems to show how federal grant money is being used. "The urgency of achieving that has not diminished — and in fact becomes more acute — with each passing day," said Sen. Daniel Akaka, top−ranking Democrat on the Senate subcommittee that oversees homeland security. Many other states are facing the same problems.
Source: http://the.honoluluadvertiser.com/article/2004/Mar/20/ln/ln1 2a.html

[Return to top]

Information and Telecommunications Sector

23. *March 20, Washington Post* — **'Witty' worm wrecks computers.** A quickly spreading Internet worm exploited a security flaw in a firewall program designed to protect PCs from online threats on Saturday, March 20, computer experts said. **The "Witty" worm writes random data onto the hard drives of computers equipped with the Black Ice and Real Secure Internet firewall products, causing the drives to fail and making it impossible to restart the PCs.** Unlike many recent worms that arrive as e−mail attachments, it spreads automatically to vulnerable computers without any action on the part of the user. **At least 50,000 computers**

have been infected so far, according to computer security firm iDefense and the SANS Institute. **Most infected computers will have to be rebuilt from scratch** unless their owners instead decide to buy new ones, said Ken Dunham of iDefense. Joe Stewart of security services company Lurhq said he expects the worm to die out over the next few hours as vulnerable computers quickly become useless hosts. A patch is available the deveoper of the firewalls, Internet Security Systems: http://xforce.iss.net/xforce/alerts/id/167
Source: http://www.washingtonpost.com/wp−dyn/articles/A11310−2004Mar 20.html

24. *March 19, CNET News.com* — **Flaw stymies Norton Internet Security.** A software component of Norton Internet Security could allow hackers to use the application as a backdoor into a person's computer system, security researchers warned Friday, March 19. The flaw occurs in an ActiveX component used by security firm Symantec's desktop security program, Norton Internet Security, according to research firm NGSSoftware. **The security hole could be used to run an attack program that would then take control of the computer that the software was trying to protect**. "The attack can be achieved either by encouraging the victim to visit a malicious Web page or placing a script within...an HTML e−mail," the advisory stated. Symantec's Antispam software has a similar issue caused by a different ActiveX component. **Fixes for the flaws can be downloaded using Symantec's LiveUpdate.**
Source: http://news.com.com/2100−7355_3−5176442.html?tag=nefd_top

25. *March 19, IDG News Service* — **Hotmail, MSN Messenger hit with another outage.** Technical problems at Microsoft Corp. for the second time within a week caused trouble for users trying to connect to Hotmail and MSN Messenger, the company said Thursday, March 19. **Users around the globe reported that they had problems signing on to the Hotmail and MSN Messenger services during about a three−hour period** from 5:00 p.m. GMT until 8:00 p.m. GMT Thursday. Microsoft in a statement said it identified an issue that caused log−on and connectivity issues on some MSN services for a portion of its customers and has since solved it. The company did not specify the scope of the problem. The outage also affected connectivity for MSN Internet Access customers, Microsoft said. **The company blames the problems on an unspecified internal problem and said it has no indication of any external causes such as cyberattacks**. Although to users the problem was essentially the same, Microsoft said that Thursday's problems are different from those that caused an approximately eight−hour outage last Friday.
Source: http://www.itworld.com/App/305/040319hotmail/

26. *March 19, eWEEK* — **Security holes uncovered in Apache.** Security researchers on Friday, March 19, uncovered **a vulnerability in the open−source Apache Web server software that could easily enable a denial of services attack.** The Apache problem is one of several reported in Version 2.0.48, and lets an attacker open a short−lived connection on a particular, rarely accessed listening socket. The software will block out all other connections until another connection comes in on the same socket. The Apache Software Foundation released update to its HTTP Server software that fixed the problem as well as several others: http://www.apacheweek.com/redirect.cgi?link=http://www.apach e.org/
Source: http://www.eweek.com/article2/0,1759,1551715,00.asp

27. *March 18, Federal Computer Week* — **Security groups call for crisis coordination center.** Two national task forces organized by the National Cyber Security Partnership on Thursday,

March 18, called for a public awareness campaign, an early warning contact network and a national crisis coordination center to improve the nation's responses to cyber vulnerabilities, threats and incidents. Establishing a national crisis coordination center by 2006 most likely would require legislation or an executive order. Guy Copeland, who led the Early Warning Task Force, said **the center would coordinate threat analyses, warnings, research and responses for critical infrastructure−sector experts and federal, state and local officials**. The early warning contact network, to be set up as early as December, would be a multichannel network housed and administered by the Department of Homeland Security's U.S. Computer Emergency Readiness Team. **Communication would occur primarily via the Internet, although task force leaders recommended having a backup means of communicating if the Internet goes down**. Reaching home users will be accomplished largely through the cooperation of Internet service providers who would keep their customers informed of cybersecurity threats and attacks, task force leaders said.
Source: http://fcw.com/fcw/articles/2004/0315/web−cybersec−03−18−04. asp

Internet Alert Dashboard

Current Alert Levels

   AlertCon: 2 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_LOVGATE.G** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	445 (microsoft−ds), 80 (www), 135 (epmap), 3127 (mydoom), 25 (smtp), 1434 (ms−sql−m), 137 (netbios−ns), 139 (netbios−ssn), 1433 (ms−sql−s), 6129 (dameware) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

28. *March 19, Associated Press* — **Small bomb explodes in car in Virginia. A small, "very low−tech" bomb damaged a junk car parked outside an auto−repair shop, and Virginia state police detonated another one found on the car's roof, authorities said Friday, March 19. The explosion in Fieldale, VA, happened shortly before 5 p.m. Thursday, March 18, in an old Volkswagen that was awaiting disposal,** Henry County Sheriff H.F. Cassell said. The resulting fire was very small, only charring the car. State police remotely detonated the second device, which was the size of a baseball, Cassell said. Two men were seen fleeing in a green truck. Cassell said authorities have suspects but wouldn't elaborate except to say, "I don't think

that this is anything related to terrorism." He said the bomb makers likely didn't mean to harm anyone, as there was no evidence of shrapnel. A nearby American Electric Power Co. substation that serves Henry County was never threatened by the explosion.
Source: http://www.newsday.com/news/nationworld/nation/wire/sns−ap−brf−car−bomb,0,4828257.story?coll=sns−ap−nation−headlines

29. *March 19, American Foreign Press/Associated Press* — **Anti−terror fight gains more urgency. The fight against terrorism is gathering steam across the world in the light of the devastating attacks on commuter trains in Madrid on March 11**. FBI director Robert Mueller spoke about the creation of an anti−terrorism alliance patterned after NATO. "We have had, upon occasion, agents from other countries full−time in the FBI building, but there are issues related to security and clearances...that a NATO−like joint intelligence centre might solve," he told members of the U.S. House of Representatives. **In the Philippines on Tuesday, March 16, an Interpol conference in Manila focused on ways to improve the global war on terror by speeding up information exchanges among countries that could thwart terrorist attacks or lead to the capture of would−be attackers.** Interpol Secretary General Ronald Noble said a communications system would give users access to an Interpol database that provides information on about 1.5 million stolen documents "which allow terrorists to move freely from one country to another." Noble said other projects under way included a database on people who have trained in suspected terrorist camps and a security alert system called the Orange Notice, in which each member country can alert others to potential criminal or terror threats.
Source: http://straitstimes.asia1.com.sg/world/story/0,4386,241009,0 0.html

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at info@us−cert.gov or visit their Web page at www.uscert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.